MAC-Kernel und Full-Disk-Zugriff in der Konsole - AMP für Endgeräte

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Fehlerbehebung in Advanced Malware Protection (AMP) für Endgeräte, um zwei MAC-Fehler zu beheben: Vollständiger Festplattenzugriff (FDA) und Kernel-Modul sind nicht autorisiert.

Unterstützt von Uriel Torres, Javier Jesus Martinez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

·Kenntnisse über Mac-Tools
·Konto mit Administratorberechtigungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco AMP für Endgeräte für MAC.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Umgebung erstellt:

- MacOS High Sierra 10.13
- MacOS 10.14 (Mojave)

Einschränkungen

Hierbei handelt es sich um einen kosmetischen Fehler bei OSX- und AMP-Anschlüssen, die auf OSV-10.4.X und Connector-Version 1.11.0 installiert sind. Das AMP-Portal zeigt eine Fehlermeldung für FDA an, und der Host zeigt an, dass FDA zulässig ist.
Bug-ID: CSCvq98799

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Wenn eine Anforderung zum Laden eines KEXT gestellt, aber noch nicht genehmigt wurde, wird die Ladeanforderung abgelehnt. MacOS High Sierra 10.13 führt eine neue Funktion ein, was bedeutet, dass der Benutzer eine Genehmigung benötigt, bevor er neu installierte Kernel-Erweiterungen (KEXTs) von Drittanbietern lädt und nur Kernel-Erweiterungen, die genehmigt wurden, auf einem System geladen werden. Der Benutzer muss die oben genannten Schritte befolgen, um den Kernel-Fehler zu beheben.
Da MACOS 10.14 (Mojave) neue Sicherheitsfunktionen für AMP für Endgeräte-Mac-Connectors einführt, müssen Sie sicherstellen, dass der AMP-Service-Daemon vollen Festplattenzugriff erhält. Ohne Genehmigung kann der AMP Connector diese Teile des Dateisystems, die durch MACOS geschützt sind, nicht schützen oder transparenter machen.

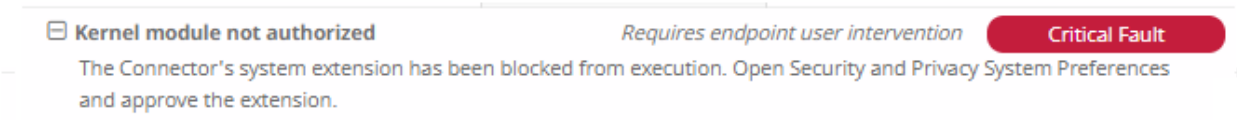
Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Konsolenfehler

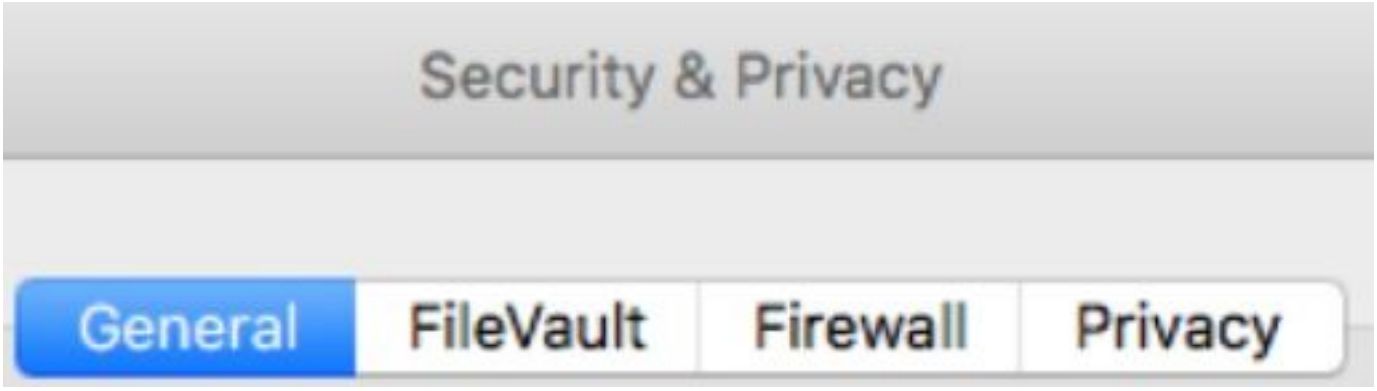
Kernel-Fehler

AMP Console zeigt den Fehler "Kernel module not authorized" (Kernelmodul nicht autorisiert) an, wenn eine Anfrage zum Laden einer Kernel-Erweiterung (KEXT) gestellt wird und es nicht genehmigt wird. Die Ladeanforderung wird abgelehnt, und macOS gibt eine Warnung aus, wie im Bild gezeigt.

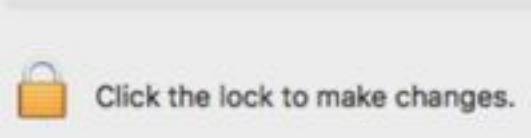


Nach dem Apple MacOS-Upgrade wurde eine offizielle Ankündigung über die Kernel-Freigabe gestartet, wie im Image gezeigt.

Um die Anschluss-Erweiterung zu aktivieren, navigieren Sie zu **System Preferences > Security & Privacy > General (Systemeinstellungen > Sicherheit & Datenschutz > Allgemein),** wie im Bild gezeigt.



Klicken Sie auf die Sperre, um KEXT zu genehmigen (nur vom Benutzer genehmigte Kernel-Erweiterungen werden auf einem System geladen), wie im Bild gezeigt.

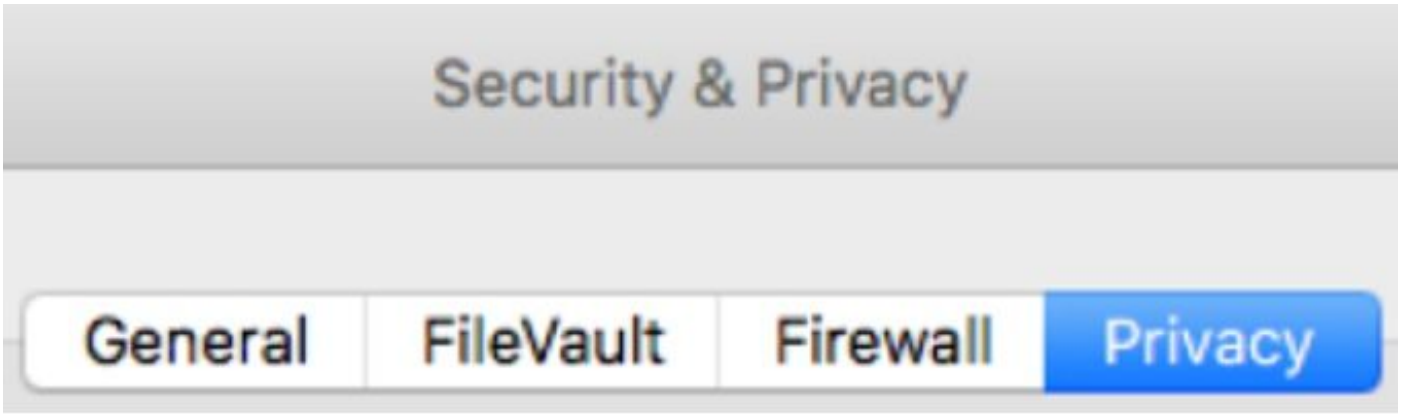


Hinweis: Die Benutzergenehmigung wird 30 Minuten nach der Warnung im Bereich für die Sicherheits- und Datenschutzeinstellungen angezeigt. Wenn das KEXT genehmigt wird, werden bei zukünftigen Auslastungsversuchen die Genehmigungsbenutzeroberfläche wieder angezeigt, es wird jedoch keine weitere Benutzerwarnung ausgelöst.

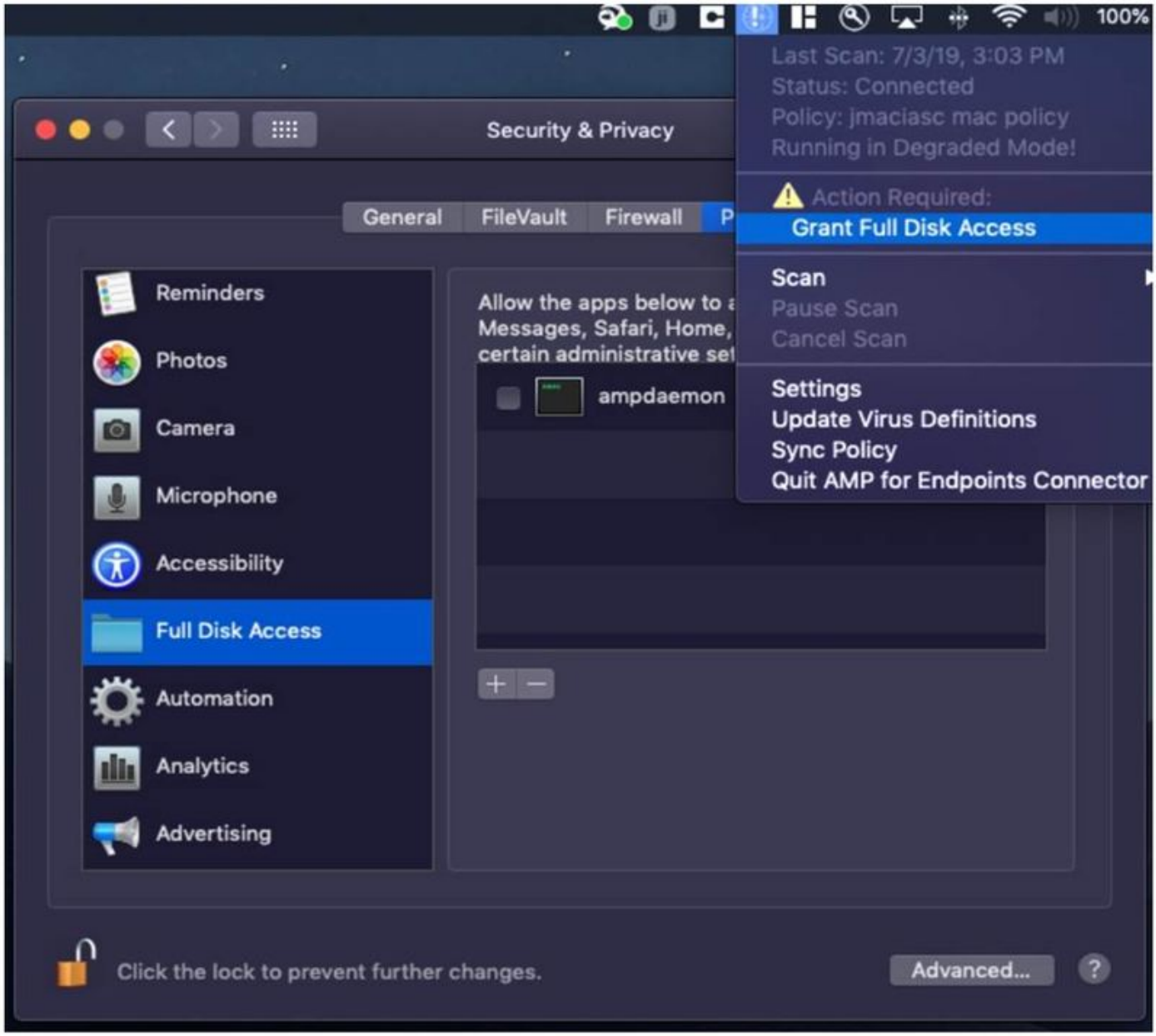
Vollständiger Festplattenzugriffsfehler

In der AMP-Konsole wird "Festplattenzugriff nicht gewährt" angezeigt, wie in der Abbildung gezeigt.

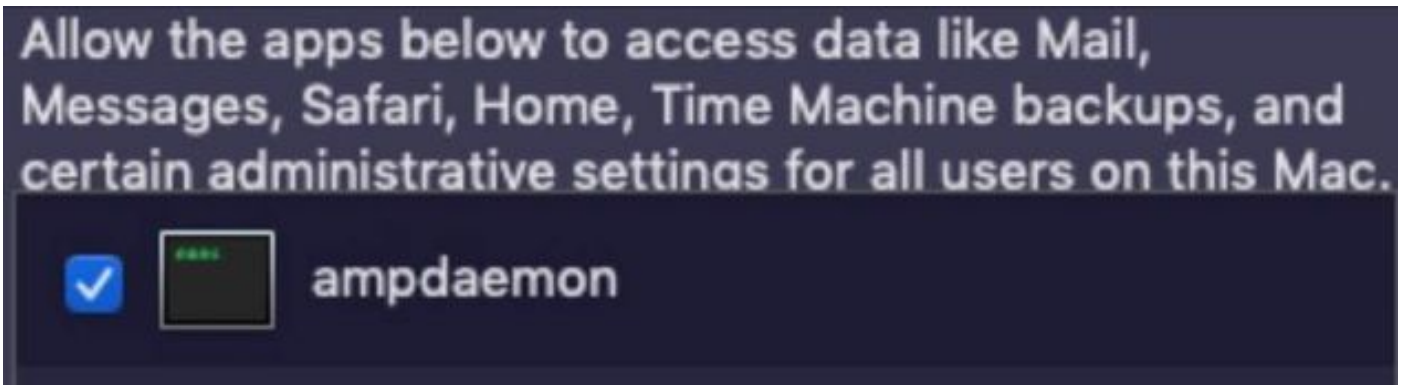
Vergewissern Sie sich, dass der vollständige Datenträgerzugriff nicht zulässig ist. Navigieren Sie zu **Systemeinstellungen > Sicherheit & Datenschutz > Datenschutz,** wie in der Abbildung gezeigt.



Um den vollständigen Festplattenzugriff auf den AMP-Anschluss zu genehmigen, navigieren Sie zu Full Disk Access (Vollständiger Festplattenzugriff), und markieren Sie den Ampdaemon-Prozess, wie im Bild gezeigt.

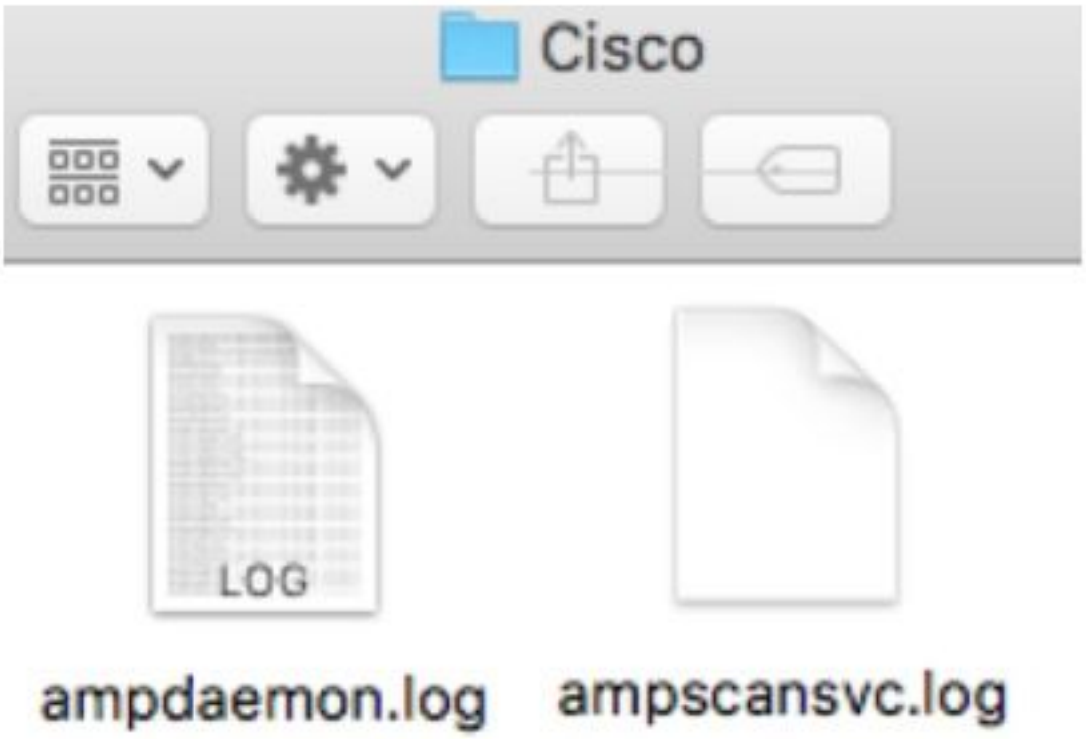


Öffnen Sie ein Terminal, beenden Sie den AMP-Dienst, und führen Sie den folgenden Befehl aus: **sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** markieren Sie das Kontrollkästchen, wie im Bild gezeigt.



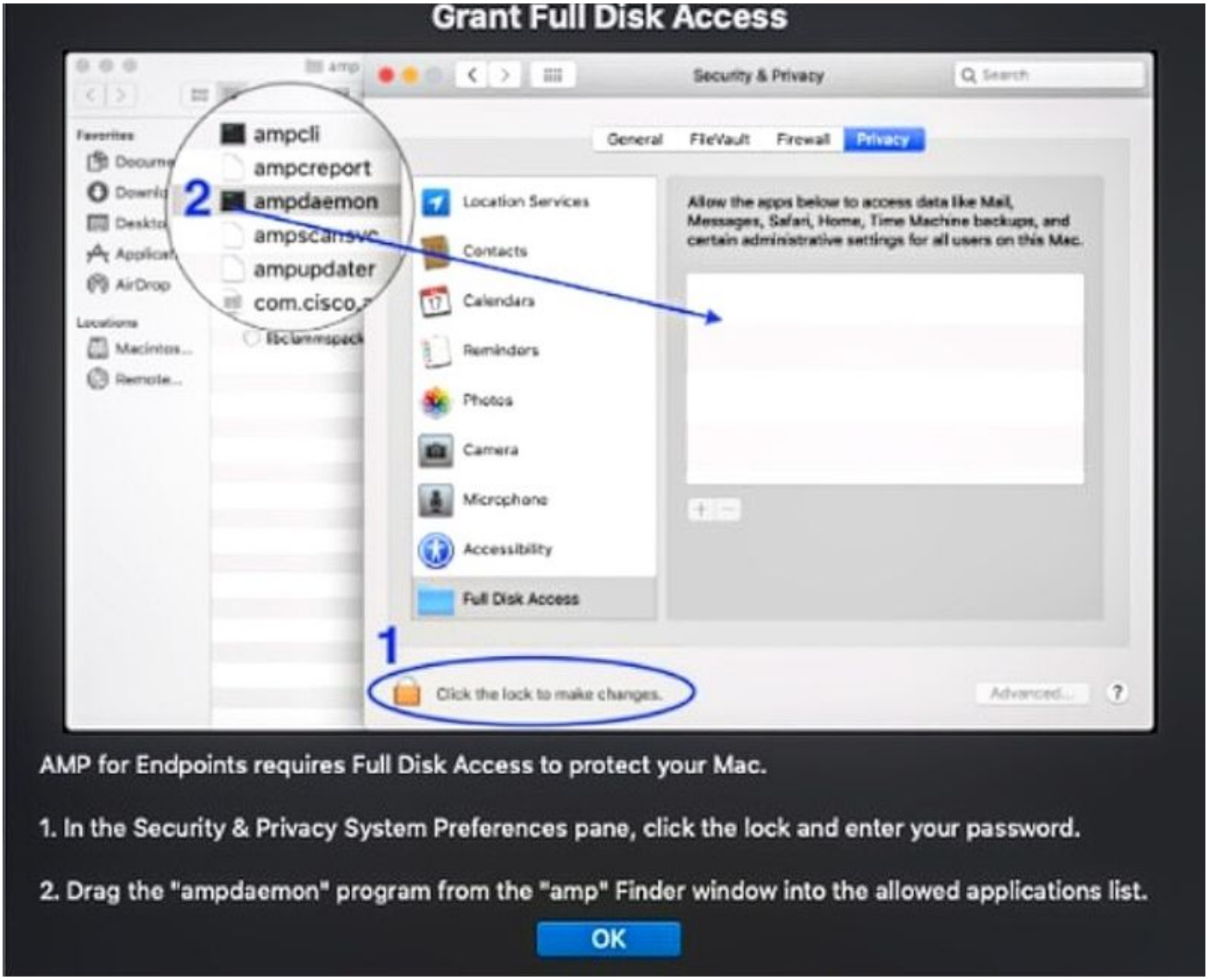
Um Cache-Probleme zu vermeiden, navigieren Sie zu **/library/logs/cisco** und löschen Sie die nächsten Dateien, wie im Bild gezeigt.

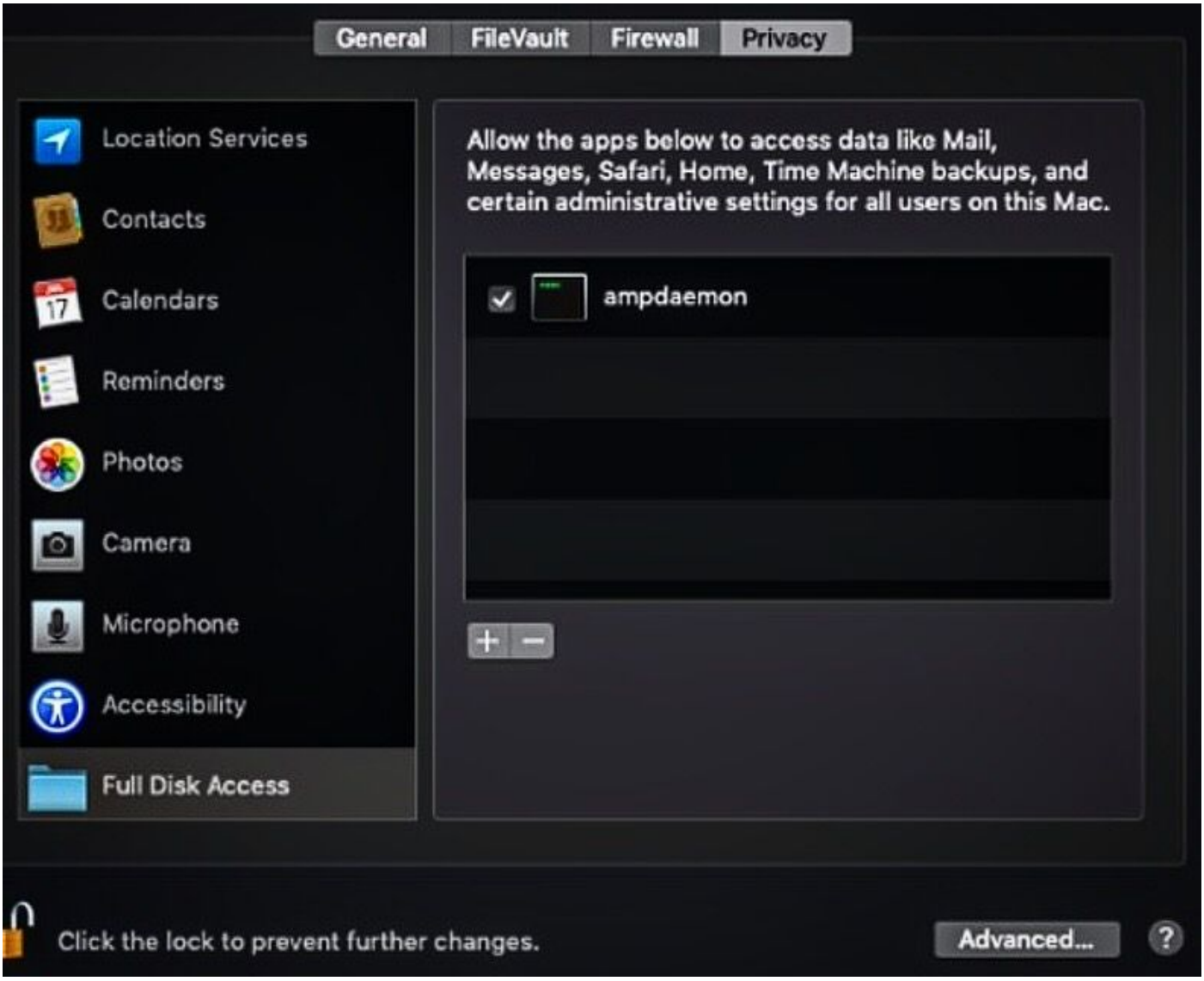
- ampdaemon.log
- ampscansvc.log



Starten Sie den Dienst mit dem Befehl **sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

> **Hinweis**: Falls Sie die Ampdeamon-Datei nicht finden können, ziehen Sie sie in die Liste Vollzugriff zulassen, und legen Sie sie in die Liste Volldatenträger zulassen, stellen Sie sicher, dass das Kontrollkästchen markiert ist, wie im Bild gezeigt.


Grant Full Disk Access
Security & Privacy
General
FileVault
Firewall
Privacy
ampcli
ampcreport
ampdaemon
ampscansvc
ampupdater
2
Location Services
Contacts
Calendars
Reminders
Photos
Camera
Microphone
Accessibility
Full Disk Access
Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.
1
Click the lock to make changes.
Advanced...
AMP for Endpoints requires Full Disk Access to protect your Mac.
1. In the Security & Privacy System Preferences pane, click the lock and enter your password.
2. Drag the "ampdaemon" program from the "amp" Finder window into the allowed applications list.
OK



Um vollständigen Festplattenzugriff zu gewähren, den Kerneln Berechtigungen und einen empfohlenen Neustart der MAC-Geräte zu gewähren, verschwindet im nächsten Taktzeitraum die gemeldete Meldung von der Konsole.